In the Claims:

Amend Claims 1, 7, 13, 17, 24,27,28,31, 34 as follows:

1   1. (currently amended) A system for authenticating an encryption

2   key of a user at a ~~remote~~-client ~~computer~~ computing device

3   that may be ~~remotely~~-networked to a server computer,

4   comprising: a decrypt engine in the ~~remote~~-client computer for

5   using a password provided by the user to decrypt in the ~~remote~~

6   client computer an encrypted data file provided by the user so

7   as to form a decrypted data file and so as to use the decrypted

8   data file to form at least port of the ~~encryption~~-key of the user,

9   without transmitting to the server either the password, the

10   encrypted data file or the decrypted data file

1   7. (~~previously~~ currently amended) A method for providing an

2   authenticated encryption key of a user at a ~~remote~~-client ~~computer~~

3   computing device that may be ~~remotely~~-networked to a server

4   computer comprising the steps of:

5   providing an encrypted data file to the ~~remote~~-client computer;

6   providing a password to the ~~remote~~-client computer; and

7   decrypting the encrypted data file in the ~~remote~~-client computer

8   using the password so as to generate an authenticated

PA1317 Amendment 020605

7

PAGE 11/26 * RCVD AT 6/2/2005 1:45:21 PM [Eastern Daylight Time] * SVR:USPTO-EFXRF-1/1 * DNIS:8729306 * CSID:250 * DURATION (mm-ss):08-36

9   encryption key of the user without transmitting the server either

10   the password or, the encrypted data file.

1   13. (currently amended) A computer accessible medium comprising

2   program instructions for providing at a ~~remote~~ client ~~computer~~

3   computing device that may be ~~remotely~~ networked to a server

4   computer an authenticated ~~encryption~~ user key ~~of a user~~,

5   comprising the steps of: using a password provided by the user

6   to decrypt in the ~~remote~~ client computer an encrypted data file

7   provided by the user so as to form a decrypted data file and so

8   as to use the decrypted data file to form at least part of an

9   authenticated ~~encryption~~ key of the user, without transmitting

10   to the server either the password, the encrypted data file or the

11   decrypted data file

1   17. (currently amended) A system for authenticating an encryption

2   key of a user, comprising: an input device at a ~~remote~~ client

3   ~~computer~~ computing device that may be ~~remotely~~ networked to

4   a server computer for receiving a password provided by the

5   user at the ~~remote~~ client computer ~~remotely~~ that may be

6   networked to a server computer; memory in the ~~remote~~ client

PA1317 Amendment 020605

8

7   ~~computer~~ computing device for storing an encrypted data file

8   including an encryption key of the user; and a decrypt engine

9   in the ~~remote~~ client computer for using the password to decrypt

10   the encrypted data file so as to form a decrypted data file and

11   so as to use the decrypted data file to generate in the ~~remote~~

12   client computer an authenticated ~~encryption~~ key of a user,

13   without transmitting to the server either the password, the

14   encrypted data file or the decrypted data file

1   24. (currently amended) A system for authenticating an encryption

2   key of a user at a ~~remote~~ client ~~computer~~ computing device

3   that may be ~~remotely~~ networked to a server computer,

4   comprising: an input device at the ~~remote~~ client computer for

5   receiving a password provided by the user; an RF smart card

6   for storing an encrypted data file, the encrypted data file

7   ~~including~~ being the encrypted source of ~~an encryption~~ a user

8   key ~~of user~~; a decrypt engine in the ~~remote~~ client computer for

9   using the password to decrypt the encrypted data file to

10   generate in the ~~remote~~ client computer an authenticated

11   ~~encryption~~ key of the user, without transmitting to the server

12   either the password, the encrypted data file or the decrypted

13   data file; memory in the ~~remote~~ client computer for storing the

14   decrypt engine.

(00060392v1)

9

1   27. (currently amended) A system for authenticating an encryption

2   key of a user at a ~~remote~~ client ~~computer~~ computing device

3   that may be ~~remotely~~ networked to a server computer,

4   comprising: an input device at the ~~remote~~ client computer for

5   receiving a password provided by the user; an RF smart card

6   for storing an encrypted data file, the encrypted data file being

7   the encrypted source of a user key ~~the encrypted data file~~

8   ~~including an encryption key of the user~~ and containing first

9   biometric data of the user; a biometric reader for generating

10   second biometric data of the user; a decrypt engine in the

11   ~~remote~~ client computer for using the password to decrypt the

12   encrypted data file so as to form a decrypted data file to

13   generate in the ~~remote~~ client computer an authenticated

14   ~~encryption~~ key of the user, if there is a probabalistic match

15   between the first biometric data and the second biometric data

16   without transmitting to the server either the password, the

17   encrypted data file or the decrypted data file;

1   28. (currently amended) A system for authenticating an encryption

2   key of a user at a ~~remote~~ client ~~computer~~ computing device

3   that may be ~~remotely~~ networked to a server computer,

4   comprising: memory in the ~~remote~~ client computer for storing

5   an encrypted encryption key; an input device at the ~~remote~~

6   client computer for receiving a password; a decrypt engine in

7   the ~~remote~~ client computer for using the password to decrypt

8   the encrypted data file so as to form a decrypted data file to

9   generate in the ~~remote~~ client computer an authenticated

10   encryption key of the user without transmitting to the server

11   either the password, the encrypted data file or the decrypted

12   data file; memory in the client computer for storing the decrypt

13   engine without transmitting to the server either the password,

14   the encrypted data file or the decrypted data file.

1   31. (currently amended) A system for authenticating an encryption

2   key of a user at a ~~remote~~ client ~~computer~~ computing device that may

3   ~~be remotely~~ networked to a server computer, comprising: memory in

4   the ~~remote~~ client computer for storing an encrypted encryption key

5   and a first biometric data of the user; an input device at the ~~remote~~

6   client computer for receiving a password; a biometric reader at the

7   ~~remote~~ client computer for generating a second biometric data of the

8   user; a decrypt engine in the ~~remote~~ client computer for comparing

9   the first biometric data of the user with a second biometric data of the

10   user and, if there is a probabilistic match, then using the password to

11   decrypt the encrypted encryption key without transmitting to the

12   server either the password, the encrypted data file or the decrypted

13   data file, data of the user.

1   34. (currently amended) A method for authenticating an encryption

2   key of a user at a ~~remote~~ client ~~computer~~ computing device that may

3   be ~~remotely~~ networked to a server computer, comprising the steps of:

4   storing an encrypted key in memory in a remote computer; receiving

5   a password provided by the user; and requiring use of the password in

6   the remote computer to decrypt the encrypted encryption key so as to

7   form a decrypted encryption key without transmitting to the server

8   either the password or the encrypted encryption key.